PARALLEL RANDOM NUMBER DETERMINATIONS FOR A STREAM CIPHER UTILIZING A COMMON S-BOX

Abstract of the Disclosure

Parallel generation of random values of a stream cipher utilizing a common S-box is provided. The generation of the values includes determining if a collision exists between accesses of the common S-box. The determination of the two sequential random values is then modified based on whether a collision exists between accesses of the common S-box. The stream cipher may be the ARC-4 cipher.